(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 44 06 602 A 1**

(51) Int. Cl.[6]:
H 04 L 9/32
H 04 M 11/00
H 04 M 3/42
G 07 C 9/00

(21) Aktenzeichen: P 44 06 602.3
(22) Anmeldetag: 1. 3. 94
(43) Offenlegungstag: 7. 9. 95

DE 44 06 602 A 1

(71) Anmelder:
Deutsche Bundespost Telekom, 53175 Bonn, DE

(72) Erfinder:
Kowalski, Bernd, Dipl.-Ing., 57072 Siegen, DE; Stolz, Helmut, Dipl.-Ing., 57080 Siegen, DE

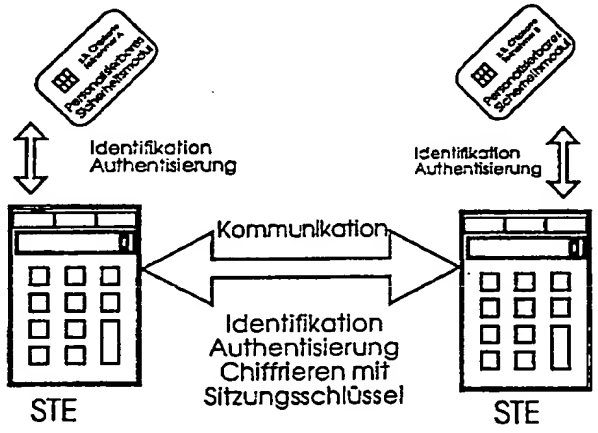
(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE	41 38 861 A1
US	52 74 699
US	52 39 583
US	52 22 140
US	52 02 921
US	46 79 226
EP	21 401 B1
EP	04 51 695 A2
EP	3 46 180 A1
SU	17 32 362 A1
SU	11 63 744 A1

BELLER,Michael,J.; et.al.: Privacy and Authenica- tion on a Portable Communications System. In: IEEE Journal on Selected Areas in Communications, Vol.11, No.6. Aug. 1993, S.821-829;
ALLERBECK,Mechthild; FISCHER,Norbert: Mobile Kom- munikation mit HICOM-Chipkarte. In: telcom report 9, 1986, H.4, S.270-273;
ARNDT,Gerhard; LUEDER,Reinhard: Bewegungsfreiheit in allen Netzen. In: telcom report 16, 1993, H.2, S.67-69;
GABEL,J.: Die Chipkarte im Funktelefonnetz C. In: ntz Bd.41, 1988, H.10, S.586-589;

(54) Sicherheitssystem zum Identifizieren und Authentisieren von Kommunikationspartnern

(57) Die erfindungsgemäße Lösung betrifft ein Sicherheitssystem, das eine eindeutige Identifizierung und Authentisierung von Kommunikationspartnern ermöglicht und somit die notwendige Sicherheit für den Austausch von vertraulichen Informationen gewährleistet.
Voraussetzung ist, daß alle Kommunikationspartner mit einem individuellen Sicherheitsmodul ausgestattet sind und über sicherheitstechnische Einrichtungen STE verfügen. Der Verbindungsaufbau wird von den STE übernommen. Dabei wird geprüft, ob beim Kommunikationspartner ebenfalls eine aktivierte STE vorhanden ist. Mit dieser STE wird ein Informationsaustausch und ein Authentikations- und Schlüsselaustauschprotokoll vorgenommen. Danach erfolgt eine persönliche Authentizierung und die Betriebsartentscheidung einschließlich evtl. erforderlicher Schlüsselvereinbarung.
Mittels der erfindungsgemäßen Lösung werden sowohl die Sicherheit der Kommunikationspartner als auch die Sicherheit des Kartenterminals in die Prüfung auf Informationssicherheit einbezogen.



DE 44 06 602 A 1

AQ

Beschreibung

Die Erfindung betrifft ein Sicherheitssystem zum Identifizieren und Authentisieren von Kommunikationspartnern der im Oberbegriff des Patentanspruch 1 näher definierten Art, welche die Informationssicherheit mit Sicherheitsmechanismen von hoher Wirksamkeit erreicht. Sie schützt insbesondere gegen die Bedrohungen:

— Verlust der Vertraulichkeit (Schutz vor unbefugter Preisgabe von Informationen)
— Verlust der Integrität (Schutz vor unbefugter Änderung von Informationen)
— Verlust der Anonymität (Schutz vor unbefugter Preisgabe der Identität).

Zusätzlich bietet ein Kommunikationssystem, das mit diesen Einrichtungen ausgestattet ist, die Möglichkeit, daß der Zugriff auf Computersysteme, die in diesem Kommunikationsnetz betrieben werden, gesichert wird.

Bestehende Kommunikationsinfrastrukturen verfügen im allgemeinen nicht über ausreichende Mechanismen, daß Kommunikationspartner sich gegenseitig eindeutig identifizieren und authentisieren können, um anschließend und vertraulich Informationen auszutauschen. Erst durch erhebliche Eingriffe in die benutzten Kommunikationssysteme können die Partner nach vorherigen Verabredungen notwendiger Parameter die Prozesse aktivieren, die z. B. durch kryptographische Verfahren, einen vertrauenswürdigeren Informationsaustausch gestatten und in der Regel noch zusätzliche Maßnahmen notwendig machen. Geeignete kryptographische Verfahren gestatten grundsätzlich eine vertrauliche Kommunikation.

Durch den Einsatz von geeigneten Sicherheitsmodulen (wie z. B. Chipkarten) ist eine Identifikation von Benutzern auf eine höchst vertrauenswürdige Weise möglich.

Geeignete Chipkarten lassen den Zugriff auf interne Funktionen und Daten nur dann zu, wenn sich ein Benutzer gegenüber der Chipkarte durch ein Merkmal oder Geheimnis (persönliche Geheimzahl, Fingerprint, etc.) eindeutig identifiziert. Für die Identifikation des Benutzers gegenüber der Chipkarte muß ein Kartenterminal verwendet werden. Auch die Sicherheit des Kartenterminals muß in die Betrachtung der Informationssicherheit einbezogen werden. Das Kartenterminal hat sich deshalb ebenfalls gegenüber der Chipkarte des Benutzers eindeutig zu identifizieren.

Mit der vorliegenden Erfindung soll ein vom Kommunikationssystem unabhängiges Sicherheitssystem geschaffen werden, das die Identifikation von Benutzern mit einer Chipkarte bei Einsatz eines Chipkartenterminals mit der gegenseitigen Authentikation von Benutzern, dem Parameteraustausch für den Einsatz kryptographischer Verfahren und deren Anwendung für den vertraulichen Informationsaustausch zwischen Kommunikationspartnern verknüpft. Dazu soll kein Eingriff in die bestehenden Kommunikationssysteme notwendig sein.

Diese Aufgabe wird erfindungsgemäß entsprechend dem Kennzeichen des Patentanspruchs 1 gelöst.

Vorteilhafte Weiterbildungen der Erfindung sind in den Kennzeichen der Patentansprüche 2 bis 8 beschrieben.

Unter Verwendung eines individuellen und personalisierbaren Sicherheitsmoduls (z. B. einer Chipkarte) und

den Sicherheitsfunktionen von sicherheitstechnischen Einrichtungen (kurz STE) wird der authentische und vertrauliche Informationsaustausch in Kommunikationssystemen, — hierzu zählen sämtliche Daten- und Computernetze im lokalen wie auch im Weitverkehrsbetrieb — für die digitale Übertragung von Daten und Sprache gewährleistet.

Die sicherheitstechnischen Einrichtungen sind gemäß dieser Erfindung in bestehende Kommunikationsinfrastrukturen als aktive Komponenten integrierbar und können zusätzlich einen gesicherten Zugriff auf vorhandene Informationssysteme gewährleisten. Für diese Informationssysteme sollen keine oder nur minimale Erweiterungen oder Konfigurationsänderungen notwendig werden.

Wichtiges technisches Merkmal der STE ist, daß Benutzer sich eindeutig mit Hilfe von personalisierten Sicherheitsmodulen identifizieren und authentisieren müssen. Es ist allerdings auch möglich, daß die Funktionalität eines personalisierten Sicherheitsmoduls in die STE integriert wird.

Nachfolgend wird die Erfindung anhand von Ausführungsbeispielen näher erläutert. In den zugehörigen Zeichnungen zeigen die:

Fig. 1 eine Identifikation und Authentisierung der personalisierbaren Sicherheitsmodule und der sicherheitstechnischen Endeinrichtungen,

Fig. 2 eine Grundstruktur einer systemunabhängigen sicherheitstechnischen Endeinrichtung bzw. Security Base und die

Fig. 3 einen Einsatz von STE und Security Base als systemunabhängige Sicherheitseinrichtungen Voraussetzung für die authentische und vertrauliche Kommunikation ist, daß alle Kommunikationspartner (Teilnehmer) mit einem individuellen Sicherheitsmodul (Chipkarte) ausgestattet sind und über eine STE verfügen.

Will ein Teilnehmer sicher mit einem Partner kommunizieren, so muß er eine gültige Chipkarte in die STE oder einen Kartenleser der STE einführen. Der Teilnehmer muß sich gegenüber der Chipkarte durch Eingabe eines persönlichen Merkmals (z. B. PIN = persönliche Identifikationsnummer) identifizieren. Die Chipkarte authentisiert sich mit einem geeigneten Verfahren gegenüber der STE und die STE authentisiert sich gegenüber der Chipkarte, so daß alle Komponenten ihre Authentizität beweisen können.

Die hierfür zum Einsatz kommende Methode kann ein sogenanntes "challenge-response" Verfahren sein, das mittels eines Chiffrieralgorithmus und eines Geheimnisses (Schlüssel) zwischen den Komponenten eine verschlüsselte Zufallszahl austauschen (Authentisierungsparameter) und dadurch der Gegenseite den Besitz des Geheimnisses beweis, ohne daß dieses selbst preisgegeben werden muß. So kann die Chipkarte eine von der STE erhaltene verschlüsselte Zufallszahl dechiffrieren und an die STE zurückschicken, womit die Chipkarte beweist, daß sie im Besitz eins Geheimnisses ist (korrekter Entschlüsselungsschlüssel) und somit ihre Authentizität beweist. Die Authentikation der STE gegenüber der Chipkarte läuft analog.

Aus Sicherheitsgründen und praktischen Erwägungen soll die STE, die systemunabhängig ist, weil sie gemäß dieser Erfindung als systemunabhängige Komponente in die bestehende Infrastruktur integriert wird, möglichst direkt zwischen der bestehenden Kommunikationseinrichtung und dem Anschluß dieser an das Kommunikationsnetz installiert werden.

Versucht nun die Kommunikationseinrichtung eine

Verbindung zu einem Partner aufzubauen, so wird die STE selbständig aktiv und schaltet sich in den Kommunikationsfluß ein. Zunächst versucht die STE Informationen mit der gegenseitigen STE des Kommunikationspartners auszutauschen.

Gelingt dies nicht, (weil die z. B. gegenseitige STE nicht aktiviert wurde oder nicht vorhanden ist), so läuft die Kommunikation in gewohnter Form ab, wobei die STE eine Warnfunktion aktiviert. Diese Warnung an den Benutzer kann auf einem Display, durch Signallampen, einem Signalton oder ähnlichem ausgeführt werden.

Wird von der STE eine gegenseitige STE erkannt, so wird mit Hilfe eines Authentikations- und Schlüsselaustauschprotokolls ein Verschlüsselungsschlüssel (Sitzungsschlüssel) für ein Chiffrierverfahren zwischen beiden STE ausgehandelt. Das für die Erfindung verwendete Authentikationsprotokoll bietet dabei die sichere gegenseitige Authentikation der Chipkarten der Kommunikationspartner, den verwendeten sicherheitstechnischen Endeinrichtungen (STE) und übernimmt den Schlüsselaustausch. Dazu werden sogenannte "publickey" Verfahren eingesetzt.

Diese Verfahren zeichnen sich dadurch aus, daß für die Verschlüsselung ein anderer Schlüssel als für die Entschlüsselung verwendet wird. Daher kann einer der beiden Schlüssel für eine Verifikation veröffentlicht werden. Die Authentizität der verwendeten öffentlichen Schlüssel wird durch die Prüfung einer elektronischen Unterschrift eines Zertifikates, das den Teilnehmerschlüssel inklusive der Teilnehmeridentität und Zusatzinformationen enthält, gewährleistet. Dieses Zertifikat wird von einer vertrauenswürdigen dritten Instanz herausgegeben, die auch als Ausgabestelle der verwendeten Sicherheitsmodule wirken kann.

Die Identität des Kommunikationspartners, basierend auf dem in die STE eingeführten Sicherheitsmodul, wird der jeweiligen Gegenseite angezeigt, so daß nur mit dem Einverständnis des STE-Benutzers eine Kommunikation mit dem Partner möglich wird. Dazu verfügt die Erfindung über eine Eingabefunktion, die entweder über das angeschlossene Kommunikationsendgerät oder direkt an der STE betätigt werden kann.

Nach dem vertrauenswürdigen Schlüsselaustausch werden die Informationen zwischen den Kommunikationspartnern von STE zu STE mit dem Sitzungsschlüssel chiffriert übertragen.

Die Kommunikationspartner, die mit Chipkarte und STE ausgestattet sind, können somit ein geschlossenes Netz innerhalb einer offenen Kommunikationsinfrastruktur bilden.

Die Erfindung kann optimal zusätzlich gemäß der Ansprüche die Möglichkeit bieten, daß durch eine oder mehrere entsprechend erweiterte STE, sogenannte Security Basis (SB), Authentifikationsinformationen und Capabilities an die Kommunikationssysteme (beliebige Endeinrichtungen in bestehenden Netzen), nach der Authentikation übertragen werden. Mit Hilfe dieser Benutzerkennungen und Capabilities kann ein Kommunikationssystem die Zugriffsrechte auch von diesen verwalteten Objekten regeln. Diese Leistung wird dadurch erbracht, daß die in der SB definierten Benutzerbzw. Teilnehmerkennungen und Capabilities gespeichert und nach dem Ablauf der oben beschriebenen Authentikationsprozedur an das Endgerät übertragen werden.

Die Erfindung sieht vor, daß ein bestehendes Kommunikationssystem mit einem Modul (Security-Dämon) ausgestattet werden kann, das die Capabilities korrekt entgegen nimmt und einer Systemverwaltung zur Weiterverarbeitung übergibt.

Eine SB kann zentrale Sicherheitsmanagementaufgaben in einem Kommunikationsnetz übernehmen, indem sie für alle Teilnehmer Capabilities verwaltet.

STE und SB verfügen über Administrationsschnittstellen, die einem autorisierten Systemverwalter Zugang für Konfigurationsmöglichkeiten gestattet. Über eine derartige Schnittstelle können auch Zertifikate für Benutzer einschließlich öffentlicher Schlüssel geladen werden. STE und SB sind Kommunikationssysteme, deren Kommunikationsfähigkeit an die jeweiligen Systemschnittstellen angepaßt werden kann. So können speziell konfigurierte STE/SB in einem z. B. lokalen Netzwerk betrieben werden, wenn die STE/SB für das verwendete Kommunikationsprotokoll mit entsprechender Schnittstelle ausgerüstet wurde. Die Authentikations- und Chiffrierverfahren als zentrale Sicherheitsmechanismen werden unabhängig von der Systemkonfiguration immer mit gleicher Sicherheit bereitgestellt.

Die Sicherheitsfunktionen der STE und SB können auch angeboten werden, wenn nicht ein Sicherheitsmodul von einem Benutzer verwendet wird, sondern ein integraler Bestandteil einer speziellen STE bzw. SB ist. Die STE und SB wirken dann in einem benutzerlosen automatischen Betrieb. Dieser Betriebsmodus wird einer Gegenstelle während der Verbindungsaufbauphase signalisiert, so daß die Gegenstelle entscheiden kann, ob sie den Verbindungswunsch ablehnt oder annimmt. Auch ist der ausschließlich automatische Betrieb zwischen Kommunikationssystemen möglich.

Jede STE und SB ist eindeutig von einer dritten Instanz personalisierbar, so daß sie durch das Authentikationsprotokoll von einer Gegenstelle eindeutig identifiziert und authentisiert werden kann.

STE und SB enthalten eine Protokollierungskomponente, mit der es für den berechtigten Benutzer möglich ist, Ereignisse, wie z. B. berechtigte und unberechtigte oder abgelehnte Verbindungsaufbauten, Konfigurationsänderungen, abgebrochene Übertragungen usw., nachträglich zu kontrollieren.

Patentansprüche

1. Sicherheitssystem zum Identifizieren und Authentisieren von Kommunikationspartnern für Verbindungen über Kommunikationsnetze mit digitaler Übertragung, **dadurch gekennzeichnet**, daß mindestens allen sicherheitsbedürftigen Kommunikationspartnern, unabhängig vom verwendeten Informationssystem, jeweils an der Schnittstelle zwischen der zu sichernden Kommunikationseinrichtung und dem Kommunikationsnetz, je eine dem Netz angepaßte Sicherheitstechnische Einrichtung (nachfolgend STE) mit Eigenschaften einer Endeinrichtung beziehungsweise eine zur Sicherheitsbasis (nachfolgend SB) erweiterte STE, ein individueller Sicherheitsmodul und ein persönliches Merkmal zugeordnet werden, daß der Verbindungsaufbau von der STE bzw. SB übernommen wird und mit einer Prüfung verbunden ist, ob beim gerufenen Kommunikationspartner ebenfalls eine aktivierte STE bzw. SB erreicht wird und mit dieser ein Informationsaustausch und ein Authentikations- und Schlüsselaustauschprotokoll vorgenommen werden kann bzw. ob ein Warnsignal zu aktivieren ist, daß erst danach eine persönliche Authentisierung und die Betriebsartenentscheidung ein-

schließlich evtl. erforderlicher Schlüsselvereinbarung durchgeführt wird.

2. Sicherheitssystem nach Anspruch 1, dadurch gekennzeichnet daß die STE bzw. SB für eine automatische Kommunikation mit einem Sicherheits-Management Center (nachfolgend SMC) vorgesehen sind.

3. Sicherheitssystem nach Anspruch 1, dadurch gekennzeichnet, daß die STE bzw. SB mit Rechtedateien versehen sind, die Einträge und evtl. Leistungsmerkmale enthalten, wer in welchen Betriebsarten und evtl. mit welchen Partnern kommunizieren kann.

4. Sicherheitssystem nach Anspruch 1, dadurch gekennzeichnet daß die STE bzw. SB über eine Protokollierungskomponente verfügen, die relevante Ereignisse aufzeichnet und kontrollfähig gestaltet.

5. Sicherheitssystem nach Anspruch 1 bis 4, dadurch gekennzeichnet daß die Rechtedateien und Protokollierungskomponenten teils lokal und teils vom SMC und teils von beiden Seiten beeinflußbar sind und daß Ereignisse an das SMC gemeldet werden.

6. Sicherheitssystem nach Anspruch 1, dadurch gekennzeichnet daß die STE/SB bzw. SMC für ein dezentrales bzw. zentrales Sicherheits- und Schlüsselmanagement mit gespeicherten Zertifikaten und Schlüsseln vorgesehen sind.

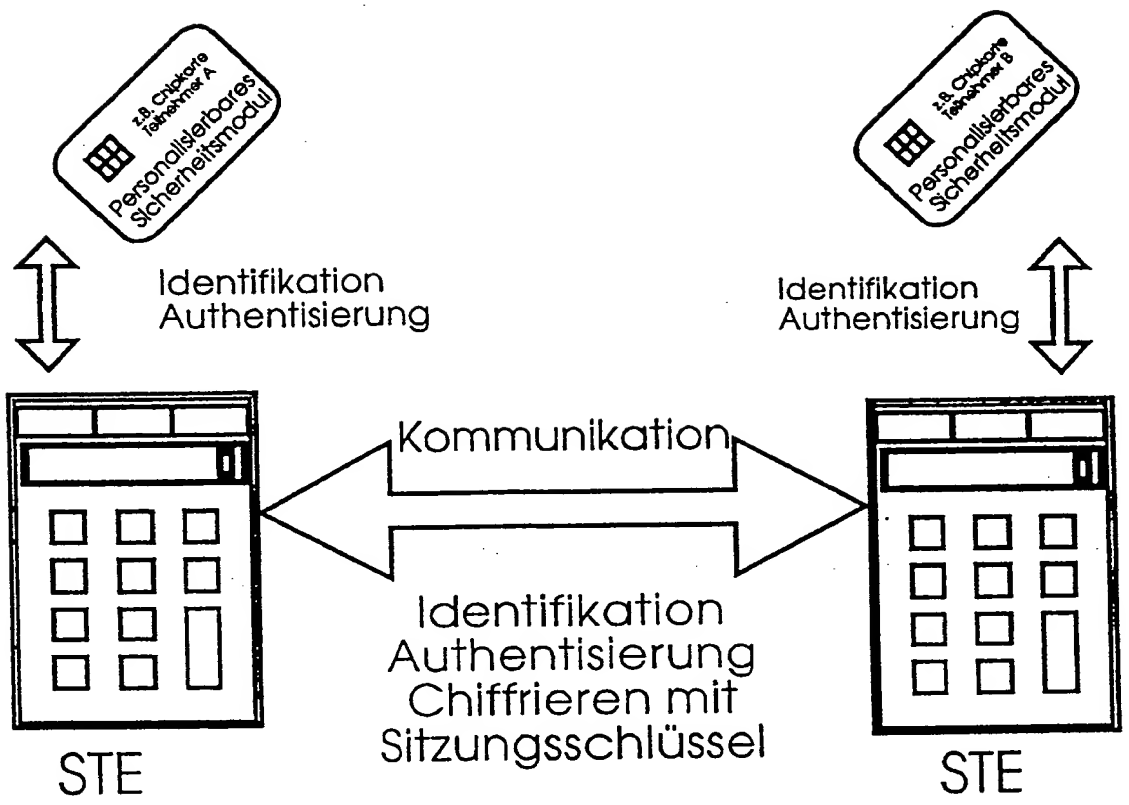
7. Sicherheitssystem nach Anspruch 1, dadurch gekennzeichnet daß die STE und SB eine digitale Unterschrift, eine Verifizierung von elektronischen Unterschriften und eine Ver- und Entschlüsselung als integrierten Dienst bereitstellen.

8. Sicherheitssystem nach Anspruch 1, dadurch gekennzeichnet daß die STE/SB und SMC mit optischen bzw. akustischen Signalisierungsmitteln versehen sind.

Hierzu 3 Seite(n) Zeichnungen

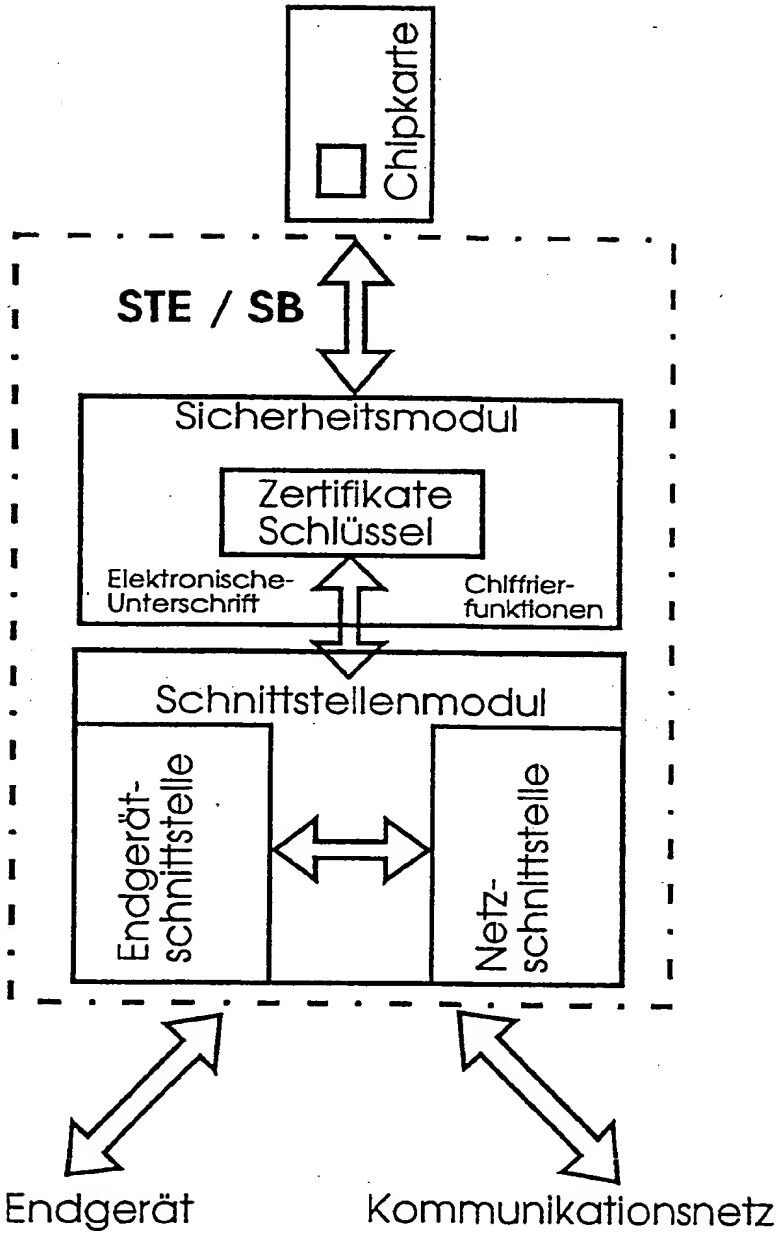
– Leerseite –

Nummer: DE 44 06 602 A1
Int. Cl.[6]: H 04 L 9/32
Offenlegungstag: 7. September 1995



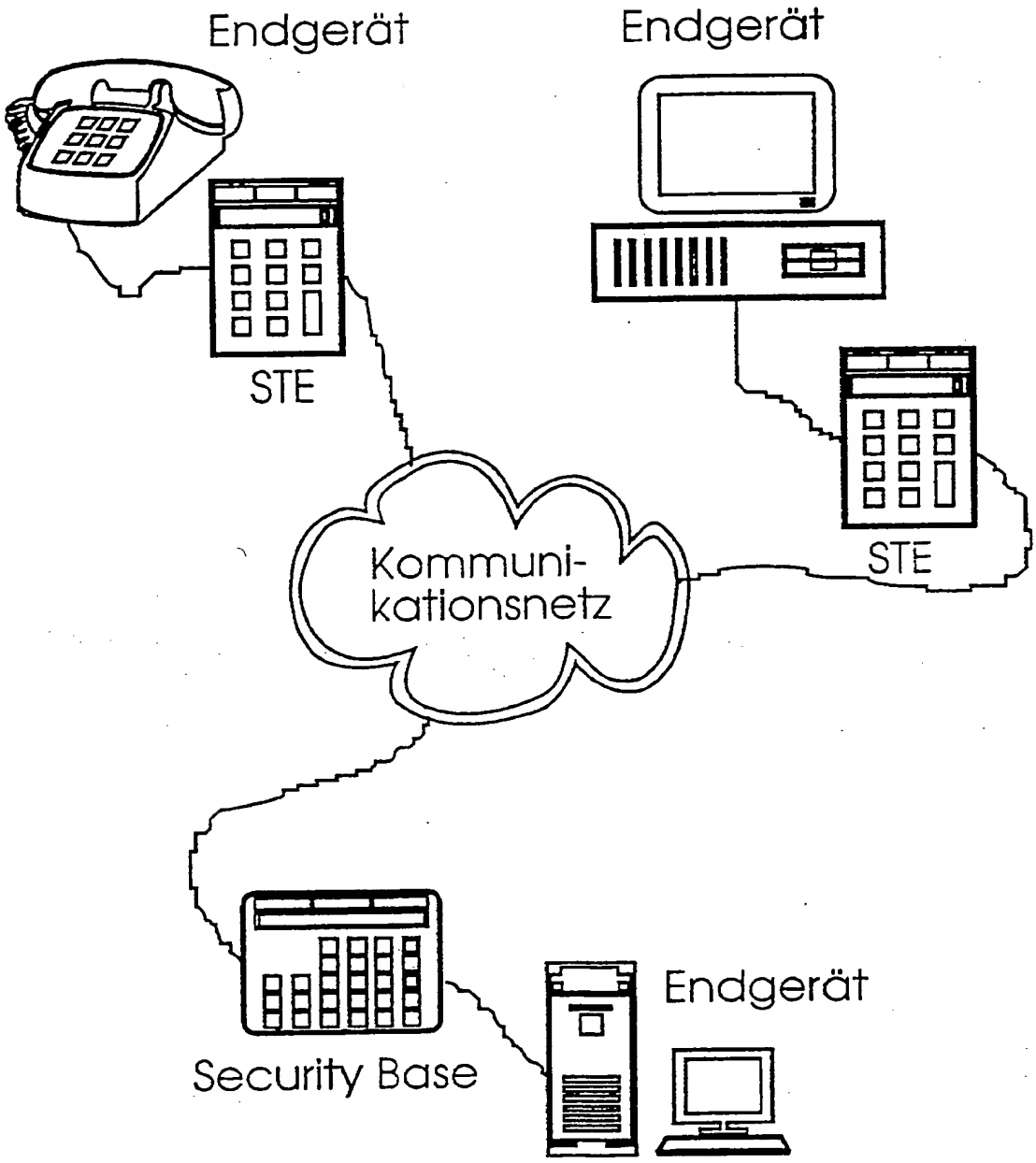
Figur 1

Nummer: DE 44 06 602 A1
Int. Cl.[6]: H 04 L 9/32
Offenlegungstag: 7. September 1995



Figur 2

Nummer: DE 44 06 602 A1
Int. Cl.[6]: H 04 L 9/32
Offenlegungstag: 7. September 1995



Figur 3